PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-344441**
(43)Date of publication of application : **29.11.2002**

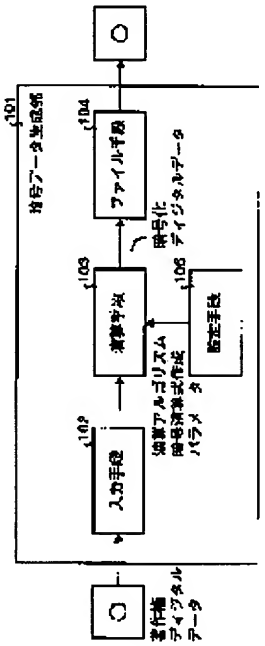
(51)Int.Cl. **H04L 9/14**
G06F 12/14
G09C 1/00

(21)Application number : **2001-142204**
(22)Date of filing : **11.05.2001**

(71)Applicant : **RICOH CO LTD**
(72)Inventor : **NASU MASAMI**

(54) DIGITAL DATA ENCRYPTION SYSTEM, DIGITAL DATA REPRODUCING DEVICE, DIGITAL DATA ENCIPHERING METHOD, DIGITAL DATA REPRODUCING METHOD AND PROGRAM FOR MAKING COMPUTER EXECUTE THE METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To protect the copyright of digital data, without imposing constraints on the use condition of a personal computer or the like, or affecting the costs of a digital data reproducing device.
SOLUTION: An input means 102 reads copyright digital data stored in a recording medium, such as CD-ROM, and an arithmetic means 103 selects a plurality of cryptographic algorithms set by a setting means 105 from a cryptographic arithmetic formula preparing parameter, and enciphers the copyright digital data according to the cryptographic arithmetic formula which is decided based on the selection. A file means 104 creates not only the enciphered digital data but also an index value and the cryptographic arithmetic formula preparing parameter in the same file, and outputs it to a flash memory. A reproduction device obtains the cryptographic arithmetic formula from the index value and the cryptographic arithmetic formula preparing parameter in the same file as that of the enciphered digital data, and reproduces digital data by carrying out corresponding decoding processing.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－344441
（P2002－344441A）
(43)公開日　平成14年11月29日(2002.11.29)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード(参考)
Ｈ０４Ｌ　9/14		Ｇ０６Ｆ　12/14	３２０Ｂ	５Ｂ０１７
Ｇ０６Ｆ　12/14	３２０		３２０Ｅ	５Ｊ１０４
		Ｇ０９Ｃ　1/00	６４０Ｄ	
Ｇ０９Ｃ　1/00	６４０	Ｈ０４Ｌ　9/00	６４１	

審査請求　未請求　請求項の数14　ＯＬ　（全 11 頁）

(21)出願番号　特願2001－142204(P2001－142204)

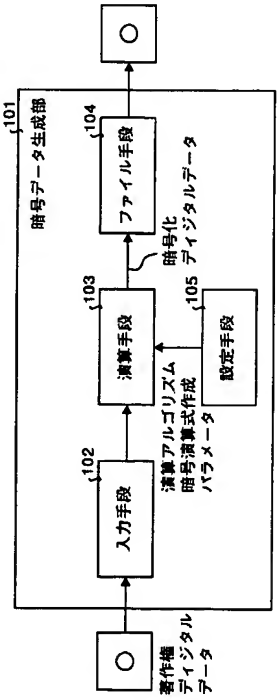
(22)出願日　平成13年５月11日(2001.5.11)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　奈須　政巳
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100104190
弁理士　酒井　昭徳

Ｆターム(参考)　5B017 AA06 BA07 CA15
5J104 AA08 AA16 AA34 EA02 EA04
EA23 PA14

(54)【発明の名称】　ディジタルデータ暗号システム、ディジタルデータ再生装置、ディジタルデータ暗号方法、ディジタルデータ再生方法およびそれらの方法をコンピュータに実行させるプログラム

(57)【要約】
【課題】　パーソナルコンピュータなどの使用条件に制約をおよぼすことなく、またディジタルデータ再生装置のコストに影響を与えずにディジタルデータの著作権を保護すること。
【解決手段】　入力手段１０２はＣＤ－ＲＯＭなどの記録媒体に格納された著作権ディジタルデータを読取り、演算手段１０３は設定手段１０５に設定された複数の暗号アルゴリズムを暗号演算式作成パラメータから選択し、この選択に基づき決定される暗号演算式にしたがって著作権ディジタルデータを暗号処理し、ファイル手段１０４は暗号化ディジタルデータとともに、インデックス値と暗号演算式作成パラメータを同一のファイルに作成しフラッシュメモリなどに出力する。再生装置は暗号化ディジタルデータと同一ファイルのインデックス値と暗号演算式作成パラメータから暗号演算式を得て対応する復号処理をして再生する。



1

【特許請求の範囲】

【請求項１】　入力されたディジタルデータを所定の暗号アルゴリズムおよび暗号演算式作成パラメータに基づき決定される暗号演算式にしたがって、暗号処理をおこなう演算手段と、

前記暗号化されたディジタルデータとともに、暗号処理に用いた暗号アルゴリズムを一意に決定可能なインデックス値と暗号演算式作成パラメータを、同一のファイルに作成出力するファイル手段と、

を備えたことを特徴とするディジタルデータ暗号システム。

【請求項２】　実際の暗号化に使用する暗号アルゴリズムがあらかじめ複数設定登録された設定手段を備え、

前記暗号処理時に所定の暗号アルゴリズムが選択可能なことを特徴とする請求項１に記載のディジタルデータ暗号システム。

【請求項３】　前記演算手段は、前記暗号処理時に、あらかじめ用意された複数の暗号アルゴリズムおよび暗号演算式作成パラメータの中から実際の暗号化に使用する暗号アルゴリズムおよび暗号演算式作成パラメータを選択し、該選択した暗号アルゴリズムおよび暗号演算式作成パラメータを用いて、暗号処理をおこなうことを特徴とする請求項１に記載のディジタルデータ暗号システム。

【請求項４】　前記演算手段は、前記暗号アルゴリズムに基づきディジタルデータの任意の場所に特定のデータ改ざん検出コードを埋め込み暗号処理を実行することにより、ディジタルデータの不正改ざんを検出可能なことを特徴とする請求項１～３のいずれか一つに記載のディジタルデータ暗号システム。

【請求項５】　前記ファイル手段は、前記暗号化ディジタルデータと同一ファイルに格納する暗号アルゴリズムのインデックス値および暗号演算式作成パラメータの記載箇所を容易に特定できない状態となるようデータ変更を施すことを特徴とする請求項１～４のいずれか一つに記載のディジタルデータ暗号システム。

【請求項６】　請求項１～５のいずれかのディジタルデータ暗号システムにより生成された暗号化ディジタルデータから著作物ディジタルデータを復号、再生するディジタルデータ再生装置であって、

前記暗号化されたディジタルデータを取り込む読み取り手段と、

前記暗号化されたディジタルデータと同一ファイル内に記載された暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を決定し、その演算式にしたがって前記暗号化されたディジタルデータの復号処理をおこなう演算手段と、

前記復号化により再現された元のディジタルデータを再生出力する再生手段と、

を備えたことを特徴とするディジタルデータ再生装置。

2

【請求項７】　前記演算手段は、前記暗号化ディジタルデータの任意の場所に埋め込まれた特定のデータ改ざん検出コードの検出の有無に基づき、ディジタルデータの改ざんの有無を判断し、不正改ざんと判断した場合には、再生しないことを特徴とする請求項６に記載のディジタルデータ再生装置。

【請求項８】　入力されたディジタルデータを所定の暗号アルゴリズムおよび暗号演算式作成パラメータに基づき決定される暗号演算式にしたがって、暗号処理をおこなう演算工程と、

前記暗号化されたディジタルデータとともに、暗号処理に用いた暗号アルゴリズムを一意に決定可能なインデックス値と暗号演算式作成パラメータを、同一のファイルに作成出力するファイル工程と、

を含んだことを特徴とするディジタルデータ暗号方法。

【請求項９】　前記演算工程は、あらかじめ用意された複数の暗号アルゴリズムおよび暗号演算式作成パラメータの中から実際の暗号化に使用する暗号アルゴリズムおよび暗号演算式作成パラメータを選択し、該選択した暗号アルゴリズムおよび暗号演算式作成パラメータを用いて、暗号処理をおこなうことを特徴とする請求項８に記載のディジタルデータ暗号方法。

【請求項１０】　前記演算工程は、前記暗号アルゴリズムに基づきディジタルデータの任意の場所に特定のデータ改ざん検出コードを埋め込み暗号処理を実行することにより、ディジタルデータの不正改ざんを検出可能なことを特徴とする請求項８，９のいずれか一つに記載のディジタルデータ暗号方法。

【請求項１１】　前記演算工程は、前記暗号化ディジタルデータと同一ファイルに格納する暗号アルゴリズムのインデックス値および暗号演算式作成パラメータの記載箇所を容易に特定できない状態となるようデータ変更を施すことを特徴とする請求項８～１０のいずれか一つに記載のディジタルデータ暗号方法。

【請求項１２】　請求項８～１０のいずれかのディジタルデータ暗号方法により生成された暗号化ディジタルデータから著作物ディジタルデータを復号、再生するディジタルデータ再生方法であって、

前記暗号化されたディジタルデータを取り込む読み取り工程と、

前記暗号化されたディジタルデータと同一ファイル内に記載された暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を決定し、その演算式にしたがって前記暗号化されたディジタルデータの復号処理をおこなう演算工程と、

前記復号化により再現された元のディジタルデータを再生出力する再生工程と、

を含むことを特徴とするディジタルデータ再生方法。

【請求項１３】　前記演算工程は、前記暗号化ディジタルデータの任意の場所に埋め込まれた特定のデータ改ざ

ん検出コードの検出の有無に基づき、ディジタルデータの改ざんの有無を判断し、不正改ざんと判断した場合には、再生しないことを特徴とする請求項１２に記載のディジタルデータ再生方法。

【請求項１４】　前記請求項８～１３のいずれか一つに記載された方法をコンピュータに実行させることを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ディジタルデータを暗号処理するディジタルデータ暗号システムと、暗号処理されたディジタルデータを再生する音楽プレイヤー、音楽再生機能を有したディジタルカメラなどを含むディジタルデータ暗号システム、ディジタルデータ再生装置、ディジタルデータ暗号方法およびその方法をコンピュータに実行させるプログラムに関する。

【０００２】

【従来の技術】近年、音楽データなどのディジタルデータの高圧縮技術、たとえば、ＭＰ３（ＭＰＥＧ３）などにより、フラッシュメモリを用いた携帯音楽プレイヤーなどのディジタルデータ再生装置が開発、発売されている。ディジタルデータ再生装置のフラッシュメモリに格納されたディジタルデータは、高圧縮技術によりデータ容量が少なく、少ないメモリ容量で長時間の音楽データを再生できるため、携帯性に優れる、消費電力が少ない、軽量化が図れるなどの利点を有している。

【０００３】

【発明が解決しようとする課題】このような、ディジタルデータ再生装置で再生されるディジタルデータ、たとえば、音楽データは著作物であるが、高圧縮されていることにより、データ容量が少ないため短時間に転送でき、またフラッシュメモリなどの小型な記録媒体に格納して容易に携帯可能なため、不正な配布および利用がなされるという問題が生じている。

【０００４】上記問題に対応するため、現在、著作物であるディジタルデータの不正な配布、使用を防止するための各種手段が提案されている。たとえば、フラッシュメモリカードを使用した携帯音楽プレイヤーは、あらかじめ著作権保護機能を有したフラッシュメモリカードを使用する構成であり、フラッシュメモリカードと、音楽プレイヤーとの間で、認証システムを使用して著作権を保護しようとするものであるが、このような方式では、ユーザーが使用するパーソナルコンピュータのオペレーティングシステム（ＯＳ）の利用条件などに大きな制約を生じる問題がある。

【０００５】また、フラッシュメモリカードを用いて再生する携帯音楽プレイヤーなどのディジタルデータ再生装置に著作権保護の方式を適用したものでは、この携帯音楽プレイヤーの電気回路の実装構成が変更となり、それにともなって開発コストが増加する問題がある。

【０００６】この発明は、上述した従来技術による問題点を解消するため、ディジタルデータの著作権を保護することができ、この保護をパーソナルコンピュータなどの使用条件に制約をおよぼすことなく、また、ディジタルデータ再生装置のコストに影響を与えずに実現できるディジタルデータ暗号システムおよびディジタルデータ再生装置の提供を目的とする。

【０００７】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、請求項１に記載の発明にかかるディジタルデータ暗号システムは、入力されたディジタルデータを所定の暗号アルゴリズムおよび暗号演算式作成パラメータに基づき決定される暗号演算式にしたがって、暗号処理をおこなう演算手段と、前記暗号化されたディジタルデータとともに、暗号処理に用いた暗号アルゴリズムを一意に決定可能なインデックス値と暗号演算式作成パラメータを、同一のファイルに作成出力するファイル手段と、を備えたことを特徴とする。

【０００８】この請求項１の発明によれば、著作物などのディジタルデータを、暗号化することによって、不正な配布を防止してディジタルデータの著作権を保護できるようになる。また、暗号化に使用する暗号アルゴリズムと、暗号演算式作成パラメータを同一のファイル内に記述するため、復号を容易におこなえるようになる。

【０００９】また、請求項２の発明にかかるディジタルデータ暗号システムは、請求項１に記載の発明において、実際の暗号化に使用する暗号アルゴリズムがあらかじめ複数設定登録された設定手段を備え、前記暗号処理時に所定の暗号アルゴリズムが選択可能なことを特徴とする。

【００１０】この請求項２の発明によれば、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズムを複数の中から選択可能であるため、暗号化のルールを複雑化でき、暗号化ディジタルデータの解読の可能性を低減化できるようになる。

【００１１】また、請求項３の発明にかかるディジタルデータ暗号システムは、請求項１に記載の発明において、前記演算手段は、前記暗号処理時に、あらかじめ用意された複数の暗号アルゴリズムおよび暗号演算式作成パラメータの中から実際の暗号化に使用する暗号アルゴリズムおよび暗号演算式作成パラメータを選択し、該選択した暗号アルゴリズムおよび暗号演算式作成パラメータを用いて、暗号処理をおこなうことを特徴とする。

【００１２】この請求項３の発明によれば、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズムを複数から選択可能であり、複数ディジタルデータの暗号化をおこなう場合に、暗号アルゴリズムと暗号演算式作成パラメータを変化させることによって、暗号化のルールをより複雑化でき、暗号化ディジタルデータの解読の可能性をより低減化できるようになる。

5

【００１３】また、請求項４の発明にかかるディジタルデータ暗号システムは、請求項１～３のいずれか一つに記載の発明において、前記演算手段は、前記暗号アルゴリズムに基づきディジタルデータの任意の場所に特定のデータ改ざん検出コードを埋め込み暗号処理を実行することにより、ディジタルデータの不正改ざんを検出可能なことを特徴とする。

【００１４】この請求項４の発明によれば、データ改ざん検出コードに基づき暗号化されたディジタルデータに対する改ざんの有無を検出でき、ディジタルデータが正規のものであるか不正改ざんされたものであるかを判断できるようになる。

【００１５】また、請求項５の発明にかかるディジタルデータ暗号システムは、請求項１～４のいずれか一つに記載の発明において、前記ファイル手段は、前記暗号化ディジタルデータと同一ファイルに格納する暗号アルゴリズムのインデックス値および暗号演算式作成パラメータの記載箇所を容易に特定できない状態となるようデータ変更を施すことを特徴とする。

【００１６】この請求項５の発明によれば、暗号ディジタルデータと同一ファイル内に記述された、暗号アルゴリズムのインデックス値および暗号演算パラメータを隠匿することができるので、暗号演算式が不正に解読されることを防止できるようになる。

【００１７】また、請求項６の発明にかかるディジタルデータ再生装置は、請求項１～５のいずれか一つに記載のディジタルデータ暗号システムにより生成された暗号化ディジタルデータから著作物ディジタルデータを復号、再生するディジタルデータ再生装置であって、前記暗号化されたディジタルデータを取り込む読み取り手段と、前記暗号化されたディジタルデータと同一ファイル内に記載された暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を決定し、その演算式にしたがって前記暗号化されたディジタルデータの復号処理をおこなう演算手段と、前記復号化により再現された元のディジタルデータを再生出力する再生手段と、を備えたことを特徴とする。

【００１８】この請求項６の発明によれば、再生装置で再生することを目的に作成され暗号化されたディジタルデータは、同一ファイル内の暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を用いて復号処理されるので、暗号処理と対になる復号処理によってのみディジタルデータを再生することができるようになり、作成したデータを不正に配布した場合にはこの再生装置やパーソナルコンピュータなどでの再生を不可にでき、ディジタルデータの著作権を保護できるようになる。

【００１９】また、請求項７の発明にかかるディジタルデータ再生装置は、請求項６に記載の発明において、前記演算手段は、前記暗号化ディジタルデータの任意の場所に埋め込まれた特定のデータ改ざん検出コードの検出の有無に基づき、ディジタルデータの改ざんの有無を判断し、不正改ざんと判断した場合には、再生しないことを特徴とする。

6

【００２０】この請求項７の発明によれば、暗号化されたディジタルデータに埋め込まれたデータ改ざん検出コードの検出の有無でディジタルデータの不正改ざんを検出することができ、この場合ディジタルデータの再生をおこなわないため不正な復号による再生を不可能にでき、ディジタルデータの著作権を保護できるようになる。

【００２１】また、請求項８の発明にかかるディジタルデータ暗号方法は、入力されたディジタルデータを所定の暗号アルゴリズムおよび暗号演算式作成パラメータに基づき決定される暗号演算式にしたがって、暗号処理をおこなう演算工程と、前記暗号化されたディジタルデータとともに、暗号処理に用いた暗号アルゴリズムを一意に決定可能なインデックス値と暗号演算式作成パラメータを、同一のファイルに作成出力するファイル工程と、を含んだことを特徴とする。

【００２２】この請求項８の発明によれば、著作物などのディジタルデータを、簡単な手順で暗号化でき、不正な配布を防止してディジタルデータの著作権を保護できるようになる。また、暗号化に使用する暗号アルゴリズムと、暗号演算式作成パラメータを同一のファイル内に記述するため、復号を容易におこなえるようになる。

【００２３】また、請求項９の発明にかかるディジタルデータ暗号方法は、請求項８に記載の発明において、前記演算工程は、あらかじめ用意された複数の暗号アルゴリズムおよび暗号演算式作成パラメータの中から実際の暗号化に使用する暗号アルゴリズムおよび暗号演算式作成パラメータを選択し、該選択した暗号アルゴリズムおよび暗号演算式作成パラメータを用いて、暗号処理をおこなうことを特徴とする。

【００２４】この請求項９の発明によれば、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズムを複数から選択可能であり、複数ディジタルデータの暗号化をおこなう場合に、暗号アルゴリズムと暗号演算式作成パラメータを変化させることによって、暗号化のルールをより複雑化でき、暗号化ディジタルデータの解読の可能性をより低減化できるようになる。

【００２５】また、請求項１０の発明にかかるディジタルデータ暗号方法は、請求項８，９のいずれか一つに記載の発明において、前記演算工程は、前記暗号アルゴリズムに基づきディジタルデータの任意の場所に特定のデータ改ざん検出コードを埋め込み暗号処理を実行することにより、ディジタルデータの不正改ざんを検出可能なことを特徴とする。

【００２６】この請求項１０の発明によれば、データ改ざん検出コードに基づき暗号化されたディジタルデータ

に対する改ざんの有無が検出でき、ディジタルデータが正規のものであるか不正改ざんされたものであるかを判断できるようになる。

【００２７】また、請求項１１の発明にかかるディジタルデータ暗号方法は、請求項８～１０のいずれか一つに記載の発明において、前記演算工程は、前記暗号化ディジタルデータと同一ファイルに格納する暗号アルゴリズムのインデックス値および暗号演算式作成パラメータの記載箇所を容易に特定できない状態となるようデータ変更を施すことを特徴とする。

【００２８】この請求項１１の発明によれば、暗号ディジタルデータと同一ファイル内に記述された、暗号アルゴリズムのインデックス値および暗号演算パラメータを隠匿することができるので、暗号演算式が不正に解読されることを防止できるようになる。

【００２９】また、請求項１２の発明にかかるディジタルデータ再生方法は、請求項８～１０のいずれかのディジタルデータ暗号方法により生成された暗号化ディジタルデータから著作物ディジタルデータを復号、再生するディジタルデータ再生方法であって、前記暗号化されたディジタルデータを取り込む読み取り工程と、前記暗号化されたディジタルデータと同一ファイル内に記載された暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を決定し、その演算式にしたがって前記暗号化されたディジタルデータの復号処理をおこなう演算工程と、前記復号化により再現された元のディジタルデータを再生出力する再生工程と、を含むことを特徴とする。

【００３０】この請求項１２の発明によれば、再生装置で再生することを目的に作成され暗号化されたディジタルデータは、同一ファイル内の暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を用いて復号処理されるので、暗号処理と対になる復号処理によってのみディジタルデータを再生することができるようになり、作成したデータを不正に配布した場合にはこの再生装置やパーソナルコンピュータなどでの再生を不可にでき、ディジタルデータの著作権を保護できるようになる。

【００３１】また、請求項１３の発明にかかるディジタルデータ再生方法は、請求項１２に記載の発明において、前記演算工程は、前記暗号化ディジタルデータの任意の場所に埋め込まれた特定のデータ改ざん検出コードの検出の有無に基づき、ディジタルデータの改ざんの有無を判断し、不正改ざんと判断した場合には、再生しないことを特徴とする。

【００３２】この請求項１３の発明によれば、暗号化されたディジタルデータに埋め込まれたデータ改ざん検出コードの検出の有無でディジタルデータの不正改ざんを検出することができ、この場合ディジタルデータの再生をおこなわないため不正な復号による再生を不可能にでき、ディジタルデータの著作権を保護できるようになる。

【００３３】また、請求項１４の発明にかかるプログラムは、請求項８～１３のいずれか一つに記載された方法をコンピュータに実行させることを特徴とする。

【００３４】この請求項１４の発明によれば、請求項８～１３に記載された方法をコンピュータに実行させることができ、コンピュータを用いてディジタルデータの暗号処理、および復号再生処理を実行できるようになる。

【００３５】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかるディジタルデータ暗号システム、ディジタルデータ再生装置、ディジタルデータ暗号方法およびその方法をコンピュータに実行させるプログラムの好適な実施の形態を詳細に説明する。

【００３６】（実施の形態１）図１は、本発明のディジタルデータ暗号システムの要部である暗号データ生成部の構成を示すブロック図である。図１において、暗号データ生成部１０１は、著作物ディジタルデータが入力される入力手段１０２と、ＣＰＵなどからなり、入力手段１０２に入力された著作物ディジタルデータに対する暗号化処理をおこなう演算手段１０３と、ハードディスク、フラッシュメモリなどからなり、演算手段１０３で暗号化された暗号化ディジタルデータをファイル化して出力するファイル手段１０４と、演算手段１０３による暗号化処理のための暗号アルゴリズム、暗号演算式作成パラメータが登録設定されている設定手段１０５によって構成される。

【００３７】入力手段１０２は、ハードディスクやＣＤ－ＲＯＭなどの記録媒体のデータを読み出すドライブ装置を用いて構成できる。ファイル手段１０４は、ハードディスクやフラッシュメモリなどの記録媒体にデータを書き込むドライブ装置を用いて構成できる。設定手段１０５は、ＲＯＭ，ＲＡＭなどの記憶装置を用いて構成することができる。以上の構成からなる暗号データ生成部１０１は、汎用のパーソナルコンピュータを用い、演算手段１０３を以下に説明する手順で暗号化処理するプログラムを実行制御して構成できる。

【００３８】つぎに、上述した暗号データ生成部による著作物ディジタルデータの暗号化手順を、図２のフローチャートにしたがって説明する。演算手段１０３は、入力手段１０２を介し入力された著作物ディジタルデータを読み出す（ステップＳ２０１）。つぎに、実際の暗号化に使用する暗号アルゴリズム（暗号演算式）を決定（選択）する（ステップＳ２０２）。

【００３９】設定手段１０５には、あらかじめ複数の暗号アルゴリズムが登録設定されており、演算手段１０３は、一つの暗号アルゴリズムを選択する。具体的には、この暗号アルゴリズムの選択は、ユーザーの操作選択により、あるいは演算手段１０３により自動選択される。

【００４０】つぎに、演算手段１０３は、選択された暗号アルゴリズムに用いる暗号演算式作成パラメータの決定をおこなう（ステップＳ２０３）。この暗号演算式作成パラメータは、演算手段１０３によって自動的に設定される。上記の暗号アルゴリズムと、暗号演算式作成パラメータの設定により、実際に暗号処理をおこなう暗号演算式ｆ（ｘ）が決定されることになる。暗号演算式ｆ（ｘ）の決定方法は、上記選択した暗号アルゴリズム内に含まれる。

【００４１】つぎに、演算手段１０３により、上記暗号演算式ｆ（ｘ）を用いて著作物ディジタルデータに対する暗号化演算を実行する（ステップＳ２０４）。以下に、暗号化の具体例を説明する。まず、暗号化対象となる著作物ディジタルデータを、ある整数の集合（Ｘ１，Ｘ２，Ｘ３…）とみなす。どのような形の整数とするかについては、暗号アルゴリズムが示す手順を適用する。たとえば、暗号対象の著作物ディジタルデータを整数の集合とし、暗号演算式ｆ（ｘ）にしたがって、それらの整数に下記演算を施す。

【００４２】Ｙ１＝ｆ（Ｘ１），
Ｙ２＝ｆ（Ｘ２），
Ｙ３＝ｆ（Ｘ３），
…
Ｙｎ＝ｆ（Ｘｎ）

【００４３】そして、上記演算後の整数の集合（Ｙ１，Ｙ２，Ｙ３，…，Ｙｎ）を作成し、演算後の整数の集合を暗号化ディジタルデータとして生成する。

【００４４】つぎに、ファイル手段１０４は、暗号データ作成に使用した暗号アルゴリズムのインデックス値、および、暗号演算式作成パラメータを、演算後の暗号化ディジタルデータ（Ｙ１，Ｙ２，Ｙ３，…Ｙｎ）とともに同一ファイル化する（ステップＳ２０５）。ファイル化された暗号化ディジタルデータは、フラッシュメモリなどの記憶媒体に書込保存される。

【００４５】この暗号化ディジタルデータの再生は、後述するが、ファイル内の所定の箇所に記載されている暗号アルゴリズムのインデックス値を読み込み、この暗号アルゴリズムのインデックス値から決定される暗号演算式作成パラメータの記述箇所を参照することで、復号に必要な情報を取得して復号演算式を作成し、その復号演算式に基づいて復号処理をおこない、再生できるようになる。

【００４６】上記の暗号化演算により作成された暗号化ディジタルデータは、本来の著作物ディジタルデータから一般的には意味をなさない形式のデータに変換される。このため、この暗号化ディジタルデータは、上述した暗号データ生成部１０１と対をなす特定の復号処理をおこなう復号装置を用いない限り、再生することができないこととなる。このような暗号化ディジタルデータは、汎用的な環境では再生、および使用できないデータであるため、不正に配布されたとしても、その不正利用を防止することができる。

【００４７】特に、暗号化時には、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズム、暗号演算式作成パラメータの組み合わせを複数の中から選択するため、暗号化のルールを複雑化でき、暗号化ディジタルデータの解読の可能性を低減化できるようになる。

【００４８】演算手段１０３は、暗号化前の著作物ディジタルデータと、暗号化後の暗号化ディジタルデータを読み出した元の記憶媒体（入力手段１０２あるいはファイル手段１０４）に対し出力し書き込む構成としてもよい。

【００４９】（実施の形態２）図３は、本発明の実施の形態２による著作物ディジタルデータの暗号化手順を示すフローチャートである。同図において、実施の形態１（図２記載）で説明した各処理と同一の処理内容には同一の符号を附して説明を省略する。

【００５０】この実施の形態２では、演算手段１０３は、上記の暗号化演算（ステップＳ２０４）の実行前に、改ざん防止データ（データ改ざん検出コード）の埋め込み処理を実行する（ステップＳ３０１）。具体的には、暗号対象となる著作物ディジタルデータの任意の場所に、特定のデータ改ざん検出コードを埋め込むものとする。このデータ改ざん検出コードを埋め込む場所、コードの個数、コードの内容に関しては、ステップＳ２０２で選択された暗号アルゴリズムによって決定される。

【００５１】そして、このデータ改ざん検出コードを埋め込んだ著作物ディジタルデータに対してステップＳ２０４で暗号演算する。これにより、暗号処理後における暗号化ディジタルデータに対するデータ改ざんの有無は、この暗号化ディジタルデータを復号し、その中のデータ改ざん検出コードを検出し、このデータ改ざん検出コードが特定の埋め込み場所、コードの個数、コードの内容に完全一致すればデータ改ざんがないと判断でき、いずれかでも不一致時にはデータが改ざんされていると判断できるようになる。

【００５２】上記実施の形態で説明したディジタルデータ暗号システムでは、暗号化ディジタルデータとともに、暗号演算式を決定する情報（暗号アルゴリズムのインデックス値と、暗号演算式作成パラメータ）が一つのファイルとして作成される構成とした。この暗号演算式を決定する情報（暗号アルゴリズムのインデックス値と、暗号演算式作成パラメータ）が、外部からファイル中の記載箇所（たとえばエリア）を容易に特定できない状態となるよう所定のデータ変更を施す処理をおこなう構成としてもよい。

【００５３】たとえば、実際の暗号演算式を決定する情報とともに、暗号演算式を決定する情報以外の不必要な情報（たとえば乱数などの無意味なデータ列）を同一フ

ァイル中に記載する。この場合、暗号演算式を決定する情報には、不必要な情報を示すデータ（たとえば上記不必要な情報の記載エリア）を付帯させる。なお、暗号化ディジタルデータの復号化処理時には、暗号演算式を決定する情報に基づき、暗号演算式を決定する情報以外の不必要な情報を削除処理する。

【００５４】（実施の形態３）つぎに、本発明のディジタルデータ再生装置の実施形態について説明する。このディジタルデータ再生装置は、上記の実施形態で説明した暗号化ディジタルデータを復号化して著作物ディジタルデータを再生する装置である。この暗号化ディジタルデータは、上述した暗号データ生成部１０１のファイル手段１０４によりファイル化し書き込んだ挿抜可能なフラッシュメモリなどの記録媒体にデータ記録されており、この記録媒体を再生装置の読み出し装置に装着して再生処理をおこなうことができる。

【００５５】図４は、本発明のディジタルデータ再生装置の構成を示すブロック図である。ディジタルデータ再生装置４０１は、上記の暗号化ディジタルデータが記録された記録媒体を読み取る読み取り手段４０２と、ＣＰＵなどからなり、読み取り手段４０２により記録媒体から読み出した暗号化ディジタルデータから元の著作物ディジタルデータを復号化処理する演算手段４０３と、演算手段４０３による復号により得られる元の著作物ディジタルデータを再生する再生手段４０４によって構成される。

【００５６】図５は、本発明のディジタルデータ再生装置によるディジタルデータ再生時のフローチャートである。ディジタルデータ再生装置４０１の読み取り手段４０２は、記録媒体に記録されたファイルを読み出す（ステップＳ５０１）。つぎに、ファイル内の所定の箇所に記載されている暗号アルゴリズムのインデックス値を読み込む（ステップＳ５０２）。つぎに、読み出した暗号アルゴリズムのインデックス値から決定される、暗号演算式作成パラメータの記述されている箇所を参照して暗号演算式作成パラメータを得る（ステップＳ５０３）。これにより、暗号化ディジタルデータの復号化処理に必要な情報を取得できる。

【００５７】つぎに、これら取得した情報（暗号アルゴリズムのインデックス値、暗号演算式作成パラメータ）に基づき復号演算式を作成する（ステップＳ５０４）。この後、これら取得した情報と同一ファイルに格納されている暗号化ディジタルデータを復号演算式に基づいて復号処理をおこなう（ステップＳ５０５）。これにより、暗号処理される前の著作物ディジタルデータを復元することができ、再生手段４０４により、著作物ディジタルデータの形式に対応した再生がおこなえるようになる（ステップＳ５０６）。

【００５８】（実施の形態４）図６は、本発明の実施の形態４による暗号化ディジタルデータの復号化手順を示すフローチャートである。同図において、実施の形態３（図５記載）で説明した各処理と同一の処理内容には同一の符号を附して説明を省略する。

【００５９】この実施の形態４では、演算手段４０３は、上記の復号処理中に、データ改ざんの有無を判断する手順を追加したものである。暗号化ディジタルデータには、任意の場所に、特定のデータ改ざん検出コードが埋め込まれており、ステップＳ５０５の復号処理後に、このデータ改ざん検出コードが検出されれば（ステップＳ６０１：Ｙｅｓ）、データ改ざんがなくデータ再生が可能と判断して再生を続ける（ステップＳ６０２）。一方、データ改ざん検出コードが検出されない場合には（ステップＳ６０１：Ｎｏ）、データ改ざんの可能性があり、少なくともデータ再生エラーと判断して再生を中止させる（ステップＳ６０３）。

【００６０】データ改ざん検出コードの検出の具体例は、たとえば、特定の埋め込み場所、コードの個数、コードの内容に完全一致すればデータ改ざんがないと判断し、いずれかでも不一致時にはデータが改ざんされていると判断する。

【００６１】図６のフローチャートにおける復号化対象の著作物ディジタルデータは、音楽データなど所定の再生時間を有するディジタルデータの例を示すものである。このようなデータ形式の場合には、暗号化ディジタルデータ全ての再生が終了するまでの期間中は（ステップＳ６０４：Ｎｏ）、上記ステップＳ５０５における復号処理と、データ改ざんの検出処理を順次おこないながら、ステップＳ５０１に復帰して暗号化ディジタルデータを継続的に読み込み処理することになる。そして、暗号化ディジタルデータ全ての再生の終了（ステップＳ６０４：Ｙｅｓ）に基づき再生にかかる処理を終了する。

【００６２】本発明では、音楽配信などに特化した高度な著作権保護方式ではなく、ディジタルデータ再生装置用に作成された著作物ディジタルデータが不正に配布された場合に再生不能とするよう暗号処理することにより、著作物ディジタルデータを保護する構成のものであり、特にユーザーの使用環境や、開発コストに影響をおよぼさずに実現できるようにしたものである。

【００６３】そして、本発明のディジタルデータ暗号化システムの各構成は、著作権ディジタルデータの暗号化処理時に任意の暗号演算式を用いて暗号化ディジタルデータを作成し、暗号化ディジタルデータを格納する同一ファイルに暗号化演算に用いた暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータをともに格納する構成であるため、汎用のコンピュータ装置を用いて著作権ディジタルデータの暗号化をＯＳなどに制約を与えず容易におこなえるものである。

【００６４】また、上記説明した本発明のディジタルデータ再生装置の各構成は、フラッシュメモリなどの半導体メモリを使用した音楽プレイヤーや、音楽再生機能を

有したディジタルカメラなどのディジタルデータ再生装置に適用することができ、これら再生装置において再生するディジタルデータの著作権を保護できるようになる。また、ディジタルデータ再生装置側では、暗号化ディジタルデータに含まれる暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づき復号化演算を実行できるので、復号化のための特別な構成が不要で装置コストを抑えてディジタルデータの著作権保護を実現できるようになる。

【００６５】上記各実施の形態では、暗号化ディジタルデータをフラッシュメモリなどの記録媒体に格納し、これを再生する構成を例に説明したが、これに限らず、コンピュータ装置にて生成された暗号化ディジタルデータをディジタルデータ再生装置に転送する構成としては、これらコンピュータ装置とディジタルデータ再生装置との間を所定のデータ伝送形式でコネクタおよびケーブルを用いた接続で伝送する構成や、インターネットなどのネットワークを介して伝送する構成とすることができ、この場合においても上記同様の作用効果を得ることができる。

【００６６】なお、本実施の形態で説明したディジタルデータの暗号化方法は、あらかじめ用意された暗号化のプログラムを汎用のコンピュータ装置で実行することにより実現することができる。このプログラムは、ハードディスク、フロッピー（登録商標）ディスク、ＣＤ－ＲＯＭ、ＭＯ、ＤＶＤなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。またこのプログラムは、上記記録媒体を介して、インターネットなどのネットワークを介して配布することができる。また、暗号化ディジタルデータの復号化についても、ディジタルデータ再生装置に適用するのみならず、復号化のプログラムを汎用のコンピュータ装置で実行することにより実現することができる。

【００６７】

【発明の効果】以上説明したように、請求項１に記載の発明によれば、入力されたディジタルデータを所定の暗号アルゴリズムおよび暗号演算式作成パラメータに基づき決定される暗号演算式にしたがって、暗号処理をおこなう演算手段と、前記暗号化されたディジタルデータとともに、暗号処理に用いた暗号アルゴリズムを一意に決定可能なインデックス値と暗号演算式作成パラメータを、同一のファイルに作成出力するファイル手段とを備えたので、著作物などのディジタルデータの暗号化によって、不正な配布を防止してディジタルデータの著作権を保護できるようになる。また、暗号化に使用する暗号アルゴリズムと、暗号演算式作成パラメータを同一のファイル内に記述するため、復号を容易におこなう復号にかかる構成を簡単に構成できる。この著作権保護は、パーソナルコンピュータなどの使用条件に制約をおよぼすことなく実現できるという効果を奏する。

【００６８】また、請求項２に記載の発明によれば、請求項１に記載の発明において、実際の暗号化に使用する暗号アルゴリズムがあらかじめ複数設定登録された設定手段を備え、前記暗号処理時に所定の暗号アルゴリズムが選択可能としたので、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズムを複数の中から選択可能であるため、暗号化のルールを複雑化でき、暗号化ディジタルデータの解読の可能性を低減化できるという効果を奏する。

【００６９】また、請求項３に記載の発明によれば、請求項１に記載の発明において、前記演算手段は、前記暗号処理時に、あらかじめ用意された複数の暗号アルゴリズムおよび暗号演算式作成パラメータの中から実際の暗号化に使用する暗号アルゴリズムおよび暗号演算式作成パラメータを選択し、該選択した暗号アルゴリズムおよび暗号演算式作成パラメータを用いて、暗号処理をおこなうので、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズムを複数から選択可能であり、複数ディジタルデータの暗号化をおこなう場合に、暗号アルゴリズムと暗号演算式作成パラメータを変化させることによって、暗号化のルールをより複雑化でき、暗号化ディジタルデータの解読の可能性をより低減化できるという効果を奏する。

【００７０】また、請求項４に記載の発明によれば、請求項１～３のいずれか一つに記載の発明において、前記演算手段は、前記暗号アルゴリズムに基づきディジタルデータの任意の場所に特定のデータ改ざん検出コードを埋め込み暗号処理を実行するので、暗号化されたディジタルデータに対する改ざんの有無を検出でき、ディジタルデータが正規のものであるか不正改ざんされたものであるかを判断できるという効果を奏する。

【００７１】また、請求項５に記載の発明によれば、請求項１～４のいずれか一つに記載の発明において、前記演算手段は、前記暗号化ディジタルデータと同一ファイルに格納する暗号アルゴリズムのインデックス値および暗号演算式作成パラメータの記載箇所を容易に特定できない状態となるようデータ変更を施すので、暗号ディジタルデータと同一ファイル内に記述された、暗号アルゴリズムのインデックス値および暗号演算パラメータを隠匿することができ、暗号演算式が不正に解読されることを防止できるという効果を奏する。

【００７２】また、請求項６に記載の発明によれば、請求項１～５のいずれか一つに記載のディジタルデータ暗号システムにより生成された暗号化ディジタルデータから著作物ディジタルデータを復号、再生するディジタルデータ再生装置であって、前記暗号化されたディジタルデータを取り込む読み取り手段と、前記暗号化されたディジタルデータと同一ファイル内に記載された暗号アルゴリズムのインデックス値、および暗号演算式作成パラ

メータに基づく暗号演算式を決定し、その演算式にしたがって前記暗号化されたディジタルデータの復号処理をおこなう演算手段と、前記復号化により再現された元のディジタルデータを再生出力する再生手段と、を備えたので、再生装置で再生することを目的に作成され暗号化されたディジタルデータは、同一ファイル内の暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を用いて復号処理され、暗号処理と対になる復号処理によってのみディジタルデータを再生することができるようになり、作成したデータを不正に配布した場合にはこの再生装置やパーソナルコンピュータなどでの再生を不可にでき、ディジタルデータの著作権を保護できる。この著作権保護は、ディジタルデータ再生装置のコストに影響を与えずに実現できるという効果を奏する。

【００７３】また、請求項７に記載の発明によれば、請求項６に記載の発明において、前記演算手段は、前記暗号化ディジタルデータの任意の場所に埋め込まれた特定のデータ改ざん検出コードの検出の有無に基づき、ディジタルデータの改ざんの有無を判断し、不正改ざんと判断した場合には、再生しないので、暗号化されたディジタルデータに埋め込まれたデータ改ざん検出コードの検出の有無でディジタルデータの不正改ざんを検出することができ、この場合ディジタルデータの再生をおこなわないため不正な復号による再生を不可能にでき、ディジタルデータの著作権を保護できるという効果を奏する。

【００７４】また、請求項８に記載の発明によれば、入力されたディジタルデータを所定の暗号アルゴリズムおよび暗号演算式作成パラメータに基づき決定される暗号演算式にしたがって、暗号処理をおこなう演算工程と、前記暗号化されたディジタルデータとともに、暗号処理に用いた暗号アルゴリズムを一意に決定可能なインデックス値と暗号演算式作成パラメータを、同一のファイルに作成出力するファイル工程と、を含んだので、著作物などのディジタルデータを、簡単な手順で暗号化でき、不正な配布を防止してディジタルデータの著作権を保護できるようになる。また、暗号化に使用する暗号アルゴリズムと、暗号演算式作成パラメータを同一のファイル内に記述するため、復号を容易におこなえるという効果を奏する。

【００７５】また、請求項９に記載の発明によれば、請求項８に記載の発明において、前記演算工程は、あらかじめ用意された複数の暗号アルゴリズムおよび暗号演算式作成パラメータの中から実際の暗号化に使用する暗号アルゴリズムおよび暗号演算式作成パラメータを選択し、該選択した暗号アルゴリズムおよび暗号演算式作成パラメータを用いて、暗号処理をおこなうので、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズムを複数から選択可能であり、複数ディジタルデータの暗号化をおこなう場合に、暗号アルゴリズムと暗号演算式作成パラメータを変化させることによって、暗号化のルールをより複雑化でき、暗号化ディジタルデータの解読の可能性をより低減化できるという効果を奏する。

【００７６】また、請求項１０に記載の発明によれば、請求項８，９のいずれか一つに記載の発明において、前記演算工程は、前記暗号アルゴリズムに基づきディジタルデータの任意の場所に特定のデータ改ざん検出コードを埋め込み暗号処理を実行するので、データ改ざん検出コードに基づき暗号化されたディジタルデータに対する改ざんの有無が検出でき、ディジタルデータが正規のものであるか不正改ざんされたものであるかを判断できるという効果を奏する。

【００７７】また、請求項１１に記載の発明によれば、請求項８～１０のいずれか一つに記載の発明において、前記演算工程は、前記暗号化ディジタルデータと同一ファイルに格納する暗号アルゴリズムのインデックス値および暗号演算式作成パラメータの記載箇所を容易に特定できない状態となるようデータ変更を施すので、暗号ディジタルデータと同一ファイル内に記述された、暗号アルゴリズムのインデックス値および暗号演算パラメータを隠匿することができ、暗号演算式が不正に解読されることを防止できるという効果を奏する。

【００７８】また、請求項１２に記載の発明によれば、請求項８～１０のいずれかのディジタルデータ暗号方法により生成された暗号化ディジタルデータから著作物ディジタルデータを復号、再生するディジタルデータ再生方法であって、前記暗号化されたディジタルデータを取り込む読み取り工程と、前記暗号化されたディジタルデータと同一ファイル内に記載された暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を決定し、その演算式にしたがって前記暗号化されたディジタルデータの復号処理をおこなう演算工程と、前記復号化により再現された元のディジタルデータを再生出力する再生工程と、を含むので、再生装置で再生することを目的に作成され暗号化されたディジタルデータは、同一ファイル内の暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を用いて復号処理され、暗号処理と対になる復号処理によってのみディジタルデータを再生することができるようになり、作成したデータを不正に配布した場合にはこの再生装置やパーソナルコンピュータなどでの再生を不可にでき、ディジタルデータの著作権を保護できるという効果を奏する。

【００７９】また、請求項１３に記載の発明によれば、請求項１２に記載の発明において、前記演算工程は、前記暗号化ディジタルデータの任意の場所に埋め込まれた特定のデータ改ざん検出コードの検出の有無に基づき、ディジタルデータの改ざんの有無を判断し、不正改ざんと判断した場合には、再生しないので、暗号化されたデ

ィジタルデータに埋め込まれたデータ改ざん検出コードの検出の有無でディジタルデータの不正改ざんを検出することができ、この場合ディジタルデータの再生をおこなわないため不正な復号による再生を不可能にでき、ディジタルデータの著作権を保護できるという効果を奏する。

【００８０】また、請求項１４に記載の発明によれば、請求項８～１３のいずれか一つに記載された方法をコンピュータに実行させるので、コンピュータを用いてディジタルデータの暗号処理、および復号再生処理を実行できるという効果を奏する。

【図面の簡単な説明】

【図１】この発明の本実施の形態にかかるディジタルデータ暗号システムの構成を示すブロック図である。

【図２】この発明の本実施の形態にかかるディジタルデータ暗号システムによる暗号処理を示すフローチャートである。

【図３】この発明の本実施の形態にかかるディジタルデータ暗号システムによる他の暗号処理を示すフローチャートである。

【図４】この発明の本実施の形態にかかるディジタルデータ再生装置の構成を示すブロック図である。

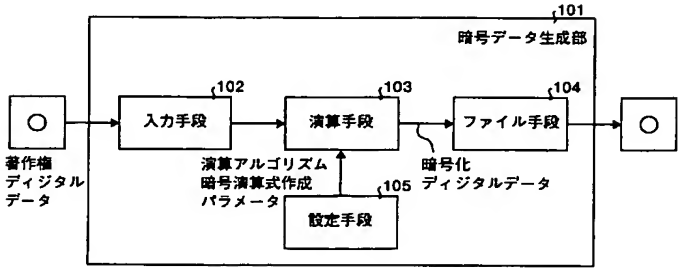
【図５】この発明の本実施の形態にかかるディジタルデータ再生装置による復号処理を示すフローチャートである。

【図６】この発明の本実施の形態にかかるディジタルデータ再生装置による復号処理を示すフローチャートである。

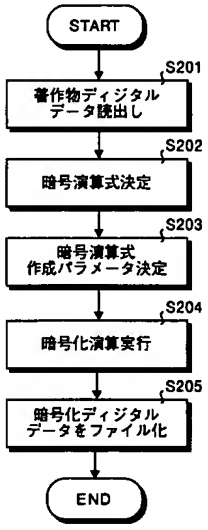
【符号の説明】

１０１　暗号データ生成部
１０２　入力手段
１０３　演算手段
１０４　ファイル手段
１０５　設定手段
４０１　ディジタルデータ再生装置
４０２　読み取り手段
４０３　演算手段
４０４　再生手段

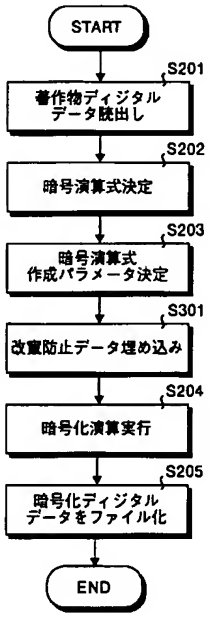
【図１】



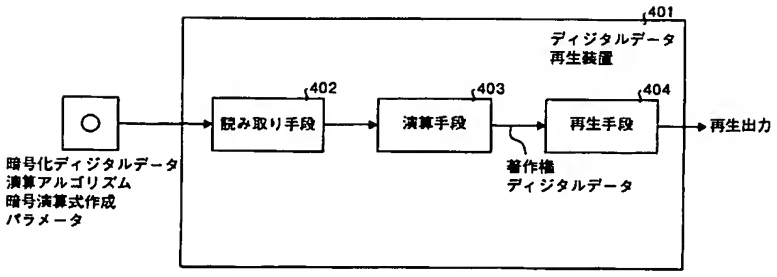
【図２】



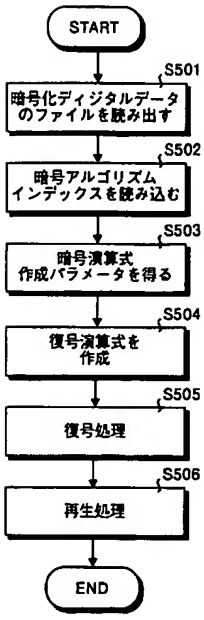
【図３】



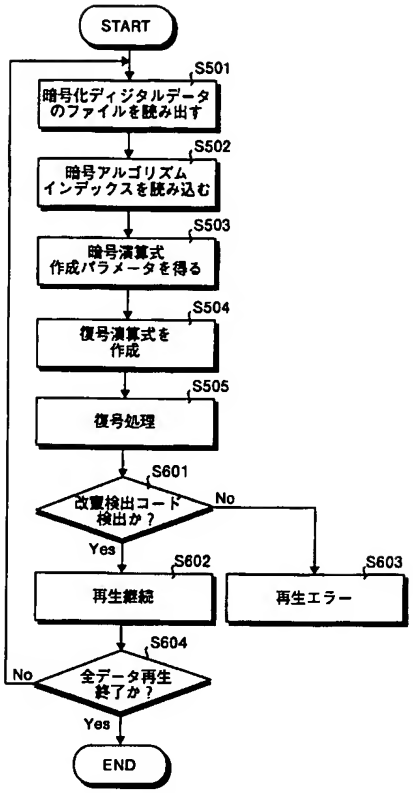
【図４】



【図５】


START
S501
暗号化ディジタルデータのファイルを読み出す
S502
暗号アルゴリズムインデックスを読み込む
S503
暗号演算式作成パラメータを得る
S504
復号演算式を作成
S505
復号処理
S506
再生処理
END

【図６】


START
S501
暗号化ディジタルデータのファイルを読み出す
S502
暗号アルゴリズムインデックスを読み込む
S503
暗号演算式作成パラメータを得る
S504
復号演算式を作成
S505
復号処理
S601
改竄検出コード検出か？
No
Yes
S602
再生継続
S603
再生エラー
S604
全データ再生終了か？
No
Yes
END